Italian Association of Aeronautics and Astronautics
XXII Conference
Napoli, 9-12 September 2013

A METHODOLOGY TO HARMONISE SAFETY, SECURITY AND COST-EFFECTIVENESS IN ATC

F. Matarese[1*], D. Dell'Amura[1], J. Fonseca[2]

[1]SESM S.c.a.r.l. a Finmeccanica Company, via Circumvallazione Esterna Loc. Pontericcio, 80014 Giugliano in Campania (NA), Italy

[2] University of Coimbra/Polytechnic Institute of Guarda, Portugal

*fmatarese@sesm.it

1 INTRODUCTION

Cyber security became an issue for many civil aviation organisations because they rely on electronic systems for critical parts of their operations, which often have safety-critical functions. With increasing air traffic, today's Air Traffic Management (ATM) system is beginning to hit its physical limits, particularly in terms of the number of aircraft that can be managed by human controllers within a given airspace. The industry has designed solutions to automate the routine part of ATM, which when put into place, will greatly increase the number of aircraft that can be managed within a given airspace, leaving the air traffic controller with the executive role rather than having to issue all the routine control instructions. However, the use of new communication methods and technologies will increase the role of cyber security and expose numerous vulnerabilities that do not exist in today's more closed, proprietary, civil aviation systems. These cyber security vulnerabilities have the potential to jeopardize civil aviation safety and efficiency.[1] In this complex scenario, it is crucial the awareness of the interaction between security, safety and cost-effectiveness. Security measures must be considered not only with regard to the level of protection deemed appropriate, but also identifying areas of synergy and potential conflicts between safety and security approaches, and highlighting cost-effectiveness opportunities within certain security and safety strategies. Given budgetary and other constraints, integrating secure/safe and cost-effective design objectives oftentimes would require compromise and tradeoffs.[2] Safety and security have different goals, which may lead to conflicts especially in the implementation of an air traffic control system. For example, the implementation of an authentication mechanism for a safety-related function may increase security since it reduces the risk of illegitimate access, but it may reduce safety since it increases the time needed to access this function. It is necessary to resolve these conflicts, not on purely intuitive decisions, but with a structured approach such that safety and security can be harmonised.[3]

2 ATM SAFETY AND SECURITY

Safety and security issues ought to be considered during the complete life cycle of an electronic system for ATM: from requirement specification, to design, operation, maintenance, and decommissioning.

In fact, safety is concerned with ensuring systematic integrity. Therefore, measures are necessary to avoid and detect faults in order to minimize risk to people. Stochastic failures

endanger system integrity. They occur during the use phase and can only be detected, but their occurrence cannot be avoided. On the contrary, systematic failures jeopardize systematic integrity during the development and use phases. They can be avoided during the development phase and detected during the use phase.

Security, on the other hand, deals with minimising risk to assets coming from threats and vulnerabilities. Countermeasures are threat and vulnerability avoidance, as well as threat control. The first one is only possible during the development phase, while threat control is performed during the use phase.[2]

2.1 ATM Safety Assessment

EUROCONTROL Safety Assessment Methodology (SAM) has been developed to reflect best practices for safety assessment of Air Navigation Services (ANSs) and to provide guidance for their application. SAM describes a generic process for the safety assessment of ANSs. It covers the complete life cycle of the ANS system, from initial planning and system definition to de-commissioning. SAM is a methodology in three main steps: Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA) and System Safety Assessment (SSA). Engineering analyses are performed in order to identify Safety Requirements for the system under evaluation.[6]

2.2 ATM Security Assessment

In the frame of DORATHEA (Development Of a Risk Assessment meTHodology to Enhance security Awareness in ATM), which is a research project co-funded by European Commission Directorate-General Home Affairs, in the frame of the Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks Programme, a Security Assessment Methodology (SecAM) for carrying out risk, threat and vulnerability assessments for ATM protection has been proposed. SecAM is an extension of ICAO ATM security guidelines and comprises three phases: Security Functional Hazard Assessment (SecFHA), Preliminary System Security Assessment (PSSecA) and System Security Assessment (SSecA). [8]

2.3 The need for a common approach

The way of integrating safety and security, chosen in the common approach, is to harmonise, not to unify, both disciplines. While unifying implies creating a new concept and methodology, the proposed harmonising approach intends to use standard concepts and methodologies from both disciplines and shows how safety and security interact.[4][5]

Even though safety and security have the same major goal, namely, risk reduction, they reduce risk because of different reasons. It is very likely that safety and security requirements on how to reduce risk differ. It could happen that these requirements contradict each other and the implementation of the requirements may also be different. Consequently, a common approach should present also a clear conflict resolution strategy, in order to identify the right system requirement (from safety or security analysis) to reduce risk.

3 SAFETY AND SECURITY ASSESSMENT

The proposed methodology is an extension of EUROCONTROL SAM and DORATHEA SecAM. It comprises three phases (see Figure 1):

- First Phase: aims at evaluating how safe and secure the system need to be in order to achieve a tolerable risk. It is a process that, evaluating system functionalities,

identifying potential Hazards and assessing the consequence of their occurrence on the system, produces the system Safety and Security Objectives. Inputs are the system functionalities and knowledge about Hazards consequences and outputs are the Safety and Security Objectives of the system.

- Second Phase: aims at evaluating if the proposed architecture is expected to achieve a tolerable risk. It is a process that produces system requirements related to Safety and Security (Safety and Security Requirements) in order to satisfy all the Safety and Security Objectives defined in the First Phase.
- Third Phase: aims at demonstrating that the system as implemented achieves a tolerable risk, i.e. satisfies the Safety and Security Objectives identified in the First Phase and the system elements meet the Safety and Security Requirements specified in the Second Phase.

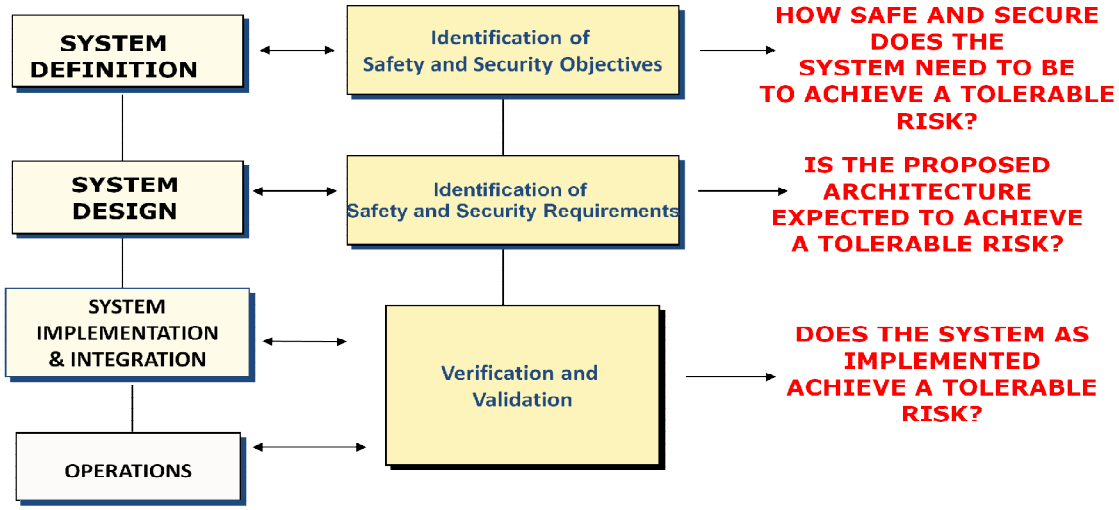

Figure 1: Safety and Security Risk Assessment Methodology Overview

3.1 First Phase: Identification of Safety and Security Objectives

The First Phase of the methodology is a top-down iterative process, starting at the beginning of the development or modification of an Air Navigation System (ANS) that aims at determining *how safe and secure the system needs to be*. A Hazard has an impact on the Safety or on the Security of the system depending on the conditions and causes (faults for Safety and threats and attacks for Security) that could lead to an accident or incident.

The steps to be performed during this phase are:

- To identify all potential Hazards associated with the system;
- To identify Hazard effects on system functionalities;
- To assess the impact of Hazard effect(s);
- To derive Safety and Security Objectives, i.e. to determine their acceptability in terms of Hazard's maximum likelihood of occurrence, derived from the impact and the maximum likelihood of the Hazard's effects.

3.1.1 Identification of Hazards

The identification of all potential Hazards is performed through the:

1. Identification of all the functionalities that the system under evaluation is expected to provide;

2. Definition of a sub-set of functionalities containing only the system's functionalities that are relevant from a safety and security point of view, i.e. the functionalities that have to be protected.
   The selection of these functionalities will take into account:
   – How critical the functionality is from a safety point of view, i.e. the loss or the corruption of such a functionality due to a fault would have a high impact on people, equipment and procedures.
   – How "attractive" is the functionality from an attacker point of view: an attacker could decide to attack a functionality on the basis of the effort needed to perform the attack in terms of costs, time needed to prepare the attack, skills required to achieve the attack, equipment required to be able to perform the attack, the likelihood of being identified during the attack.
3. Definition of all the potential Hazards as any condition, event, or circumstance which could lead to the loss or the corruption of such functionalities.

3.1.2 Identification of Hazard's effect

In order to classify the impact of Hazards, a classification scheme is adopted. All the possible consequences of the Hazard on the system are identified and the impact of these consequences are established. This impact is a number from 1 to 5 as reported in Table 1.

To obtain this evaluation, the impact of the Hazard's effect(s) must be evaluated on each of the Areas of Impact.[7][8]

	5	**4**	**3**	**2**	**1**
Impact Areas	**Catastrophic**	**Critical**	**Severe**	**Minor**	**No impact / NA**
1:Personnel, Aircrafts and Operations	Fatalities Catastrophic accidents, mid-air Collisions, collisions on the ground between two aircraft, Controlled Flight Into Terrain, total loss of flight control.	Multiple Severe injuries Large reduction in separation, without crew or ATC fully controlling the situation.	Severe injuries Large reduction in separation with crew or ATC controlling the situation and able to recover.	Minor injuries Increasing workload of the air traffic controller or aircraft flight crew.	No injuries No hazardous condition i.e. no immediate direct or indirect impact on the operations
2:Capacity	Loss of 60%-100% capacity	Loss of 60%-30% capacity	Loss of 30%-10% capacity	Loss of up to 10% capacity	No capacity loss
3:Performance	Major quality abuse that makes multiple major systems inoperable	Major quality abuse that makes major system inoperable	Severe quality abuse that makes systems partially inoperable	Minor system quality abuse	No quality abuse
4:Economic	Bankruptcy or loss of all income	Serious loss of income	Large loss of income	Minor loss of income	No effect

	5	4	3	2	1
Impact Areas	**Catastrophic**	**Critical**	**Severe**	**Minor**	**No impact / NA**
5:Branding	Government & international attention	National attention	Complaints and local attention	Minor complaints	No impact
6:Regulatory	Multiple major regulatory infractions	Major regulatory infraction	Multiple minor regulatory infractions	Minor regulatory infraction	No impact
7:Environment	Widespread or catastrophic impact on environment	Severe pollution with long term impact on environment	Severe pollution with noticeable impact on environment	Short Term impact on environment	Insignificant

Table 1: Areas of Impact

The final impact value for each Security Hazard's effect will be the maximum impact level from this evaluation.

3.1.3 Safety and Security Objectives Identification

The Safety and Security Objectives specify, for each identified Hazard, the maximum tolerable likelihood of its occurrence, given its assessed impact. In particular, it is linked to the tolerability of a loss or corruption of a functionality due to a fault or an attack.

For each identified Hazard, the Risk associated to it will be evaluated as follows:

$$Risk = L_h * I_c \quad (1)$$

Where:

- L_h indicates the likelihood of the Hazard;
- I_c indicates the impact of the consequence on the system (people, procedures, equipment).

The Risk Classification Scheme (see Table 2) is used in order to fix the maximum likelihood of a Hazard, given its assessed Impact, in order to achieve a ***tolerable risk***.

The class of likelihood is defined as follows:

- **Very Frequent**: Likely to occur often;
- **Frequent**: Likely to occur several times;
- **Occasional**: Likely to occur sometime;
- **Rare**: Unlikely but may occur exceptionally;
- **Extremely Rare**: Unlikely to occur during the lifetime of the system.

		LIKELIHOOD OF OCCURRENCE				
		1 Extremely Rare	2 Rare	3 Occasional	4 Frequent	5 Very Frequent
IMPACT CLASSES	5 Catastrophic					
	4 Critical					
	3 Severe					
	2 Minor					
	1 No impact					

Acceptable | Tolerable | Unacceptable

Table 2: Risk Classification Scheme

3.2 Second Phase: Identification of Safety and Security Requirements

The objective of the Second Phase is to evaluate *if the proposed architecture is expected to achieve a tolerable risk*. It is a top-down iterative process, conducted during the System Design phase of the system life cycle. It is performed for a new system or each time there is a change to the design of an existing system. In the second case, the purpose is to identify the impact of such a change on the architecture and to ensure the ability of the new architecture to meet either the same or new Safety/Security Objectives. The essential pre-requisite is a description of the high level functions of the system. This Second Phase aims at deriving the Safety and Security Requirements for each individual system element under evaluation (People, Procedure and Equipment), in order to satisfy the Safety and Security Objective of the system.

The Second Phase starts with the Identification of all the Assets that provide the functionalities associated to the Safety and Security Objectives, identified during the First Phase.

According to [9] the Assets are classified as:

- *Primary assets*: they are the intangible activities, information and services that contribute to have the functionalities of the system to be protected (the ones specified in the Security Objectives).
- *Supporting assets*: they are the physical entities which enable the primary assets. They are of various types, e.g., hardware, software, operating systems, business applications, networks, storage media, relays, communication interfaces, personnel, sites, premises, utilities, subcontractors, authorities and organisations.

The apportion of Safety and Security Objectives into Safety and Security Requirements allocated to the system elements, is performed through two analyses:

- Fault and Attack Tree Analysis (FATA): it is a functional analysis that aims at identifying the logical combination of consequences coming from faults and attacks, leading to the non-fulfilment of the safety and security objectives. The focus is on the consequences on Primary Assets. The output of this analysis will be the list of faults and attacks that can impact on a given Safety or Security Objective (linked to one or more Primary Asset) with an assigned likelihood.
- Failure Mode and Vulnerability Effects Analysis (FMVEA): it is a physical analysis and aims at evaluating if the Supporting Assets linked to given Safety or Security Objectives are vulnerable to the identified failures and threats.

The combination of FATA and FMVEA analyses allows the identification of how critical are the Supporting Assets and consequently to define the Countermeasures in a cost-effective way. The Countermeasures are traced to the System Requirements that become ***Safety and Security Requirements.***

Figure **2** shows an overview of the process.

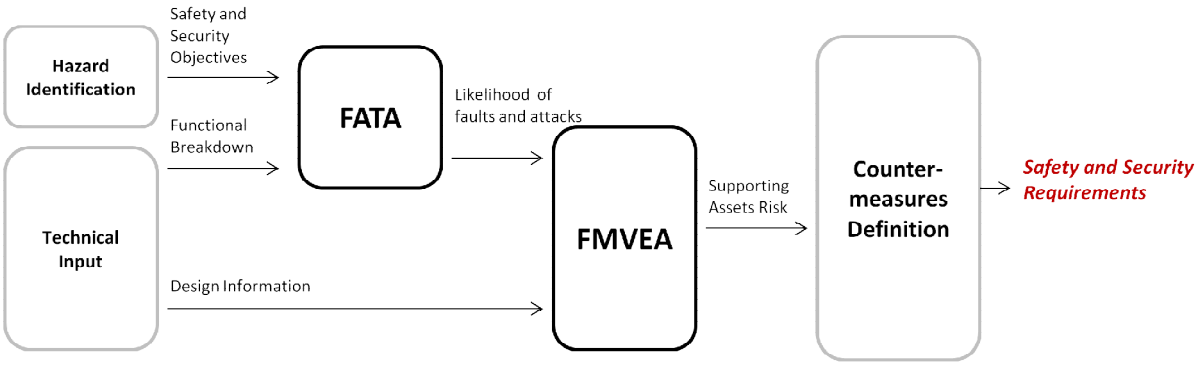

Figure 2: Safety and Security Requirements identification process

3.2.1 Fault and Attack Tree Analysis (FATA)

FATA is performed starting from the identification of credible system hazards, classified according to their severity of effects in the First Phase.

A tree is developed for each Top Event (Safety and Security Objective) identified. A tree is a model that graphically and logically represents the various combinations of possible failures and events occurring in a system that lead to a failure condition at the top.

Once the FATA is performed, starting from the likelihood assigned to the Safety or Security Objective, the likelihood to be assigned to each element in the diagram is determined by applying a top down process. In this way, it is possible to apportion the requirements coming from the Safety and Security Objectives to physical components functionalities, thus allowing a direct link of these requirements to the physical components failures that affect these functions, by performing a dedicated FMVEA.

3.2.2 Failure Mode and Vulnerability Effects Analysis (FMVEA)

FMVEA is carried out on physical components in order to identify possible failure modes, vulnerabilities, their effects at different levels, their connection to FATA, their severity, their possible countermeasures and the associated Safety and Security System Requirements.

The input of this analysis will be the design information of the system that allows establishing which Supporting Assets support the Primary Assets that provide the functionality associated to a given Safety and Security Objective.

FMVEA is a table as follows:

Supporting Assets	**Failure Mode and Vulnerability**	**Causes and Threats**	**Effect(s)**	**Likelihood**	**Safety and Security Measures**	**Likelihood after mitigation**
Name of the physical component	Failure Mode and Vulnerability of the supporting asset	Causes and Threats that exploit the vulnerability of the Supporting Asset	The consequences are related to the impact on the Primary Asset(s), supported by the associated physical component, as identified through FATA	Likelihood associated to the effect on Primary Asset, as identified through FATA	Possible measures to be applied to the Supporting Asset in order to mitigate the risk	The resulting likelihood after the application of the Safety and Security Measures

Table 3: FMVEA

3.2.3 Conflict resolution strategy

Conflict resolution is needed whenever different safety and security requirements are identified as measures to reduce a risk, which are potentially in contrast one to the other.

The first step to follow is to specify the conflict resolution policy. It is a set of rules determined by the engineer that are used to resolve conflicts. Depending on the field of application, the resolution policy may prefer safety or security aspects. The rules can apply not only to the complete system or technology but also to single entities (e.g., nodes) or even software parts (e.g., safety- and security-related protocol stacks).

The second step to follow is to group the safety and security requirements into three groups:

- detective: detection of faults and attacks;
- preventive: guard against systematic faults and attacks;
- corrective: response to a fault and attack.

While detective safety and security requirements do not have any impact on the system or entities or software parts, preventive and corrective requirements do. Thus, these two groups of requirements are subject to investigation in the conflict resolution.

Finally, the third step consists of the conflict resolution itself, it is performed by taking each conflicting preventive or corrective safety and security requirement and applying the conflict resolution policy (defined at step one). In the end, a conflict-free set of requirements is available.

3.3 Third Phase: Verification and Validation

Verification and Validation is the last phase of the methodology. This phase aims at evaluating *if the implemented architecture achieves a tolerable risk.* It is a top-down iterative process led during system integration, validation and on-site acceptance. The process

produces assurance that the Safety and Security Objectives are satisfied and that system elements meet their Safety and Security Requirements.

The objective of the Third Phase is to collect evidences and to provide assurance that:

- each system (people, procedure, equipment) element as implemented meets its Safety and Security Requirements;
- the system as implemented satisfies its Safety and Security Objectives throughout its operational lifetime (till decommissioning);
- the system satisfies users expectations with respect to Safety and Security;
- the system achieves a tolerable risk.

The correct implementation of Safety and Security Measures will be demonstrated through Verification and Validation activities.

4 CASE STUDY APPLICATION: CONTROLLER-PILOT DATA LINK COMMUNICATIONS SYSTEM

The Air Ground Datalink (AGDL) communication system has been selected to validate the methodology.

In particular the CPDLC application provides a means of communication between the controller and pilot, using data link for ATC communication. Then CPDLC is a mean of digital communication between aircraft and ATCO, allowing data exchange in digital text format.

There are two types of CPDLC messages:

- Downlink messages, which are CPDLC messages sent from aircraft;
- Uplink messages, which are CPDLC messages sent from a ground system.

The CPDLC application is used by the following services[10]:

- **ATC Communication Management (ACM)** service provides automated assistance to the aircrew and current and next controllers for conducting the transfer of ATC communications. The ACM Service encompasses the transfer of all controller/aircrew communications, both the voice channel and the data communications channel used to accomplish the ACM Service. The ACM service is completed prior to using any other CPDLC service.
- **ATC Clearance (ACL)** for exchanging clearances and requests between the current data authority ATSU and flight crew. An aircraft under the control of an ATSU transmits reports, makes requests and receives clearances, instructions and notifications. The ACL service describes the dialogue procedures to be followed to perform these exchanges via air/ground data communications. The service description states the exchanges that could be conducted via data communications, the rules for the combination of voice and data link communications and abnormal mode requirements and procedures.
- **ATC Microphone Check (AMC)** for instructing pilots to check the aircraft is not blocking a given voice channel. The AMC service allows a controller to send an instruction to all CPDLC equipped aircraft in a given sector, at the same time, in order to instruct flight crews to verify that their voice communication equipment is not blocking the sector's voice channel. This instruction will be issued only to those aircraft for which the controller currently has responsibility
- **Departure Clearances (DCL)** for exchanging departure clearance, request and start up combined messages between the current ATSU and grounded aircraft to

prepare its departure. Where local procedures or flight category require, flights intending to depart from an airport must first obtain a departure clearance from the C-ATSU. The process can only be accomplished if the flight operator has filed a flight plan with the appropriate ATM authority. The DCL Service provides automated assistance for requesting and delivering departure information and clearance, with the objective of reducing aircrew and controller workload and diminishing clearance delivery delays.

4.1 First Phase: Identification of Safety and Security Objectives

An analysis of CPDLC functionalities is performed in order to identify Hazards. According to the classification of effects, Safety and Security Objectives are identified:

Safety and Security Objectives	Description
SSO-1	The likelihood of out-of-sequence CPDLC message shall be less than Occasional
SSO-2	The likelihood of failure to exchange CPDLC messages or denial of CPDLC Services shall be less than Extremely Rare
SSO-3	The likelihood of loss of integrity or corrupted CPDLC messages exchange shall be less than Rare
SSO-4	The likelihood of non-reception or theft of a CPDLC message shall be less than Rare
SSO-5	The likelihood of reception of an unexpected or fake CPDLC message shall be less than Rare

Table 4: CPDLC Safety and Security Objectives

4.2 Second Phase: Identification of Safety and Security Requirements

FATA is performed in order to analyse Primary Assets potentially affected by the identified Safety and Security Objectives.

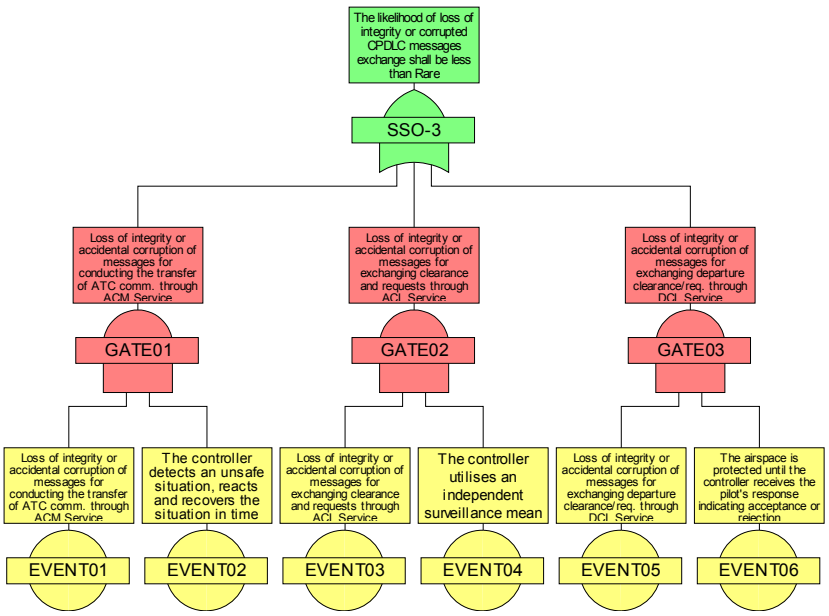

Figure 3: FATA example

FMVEA is performed in order to analyse Supporting Assets potentially affected by the identified Safety and Security Objectives and to identify Safety and Security Requirements.

Supporting Assets	**Failure Mode and Vulnerability**	**Causes and Threats**	**Effect(s)**	**Likelihood**	**Safety and Security Measures**	**Likelihood after mitigation**
Controller Working Position (CWP)	Unsecured protection of integrity of data	Corruption of data	If the message is related to a clearance, the flight crew and ground are out of sync	Rare	Requirements for ensuring authenticity and protecting message integrity	Occasional
CWP	Lack of data validity checks	Corruption of data	If the message is related to a clearance, the flight crew and ground are out of sync	Rare	Semantic and Syntactic checks shall be incorporated to detect any corruption of information through processing errors or deliberate acts	Occasional
Dual Data Link Server (DLS)	Unsecured protection of integrity of data	Corruption of data	The situation will develop slowly: not all aircraft will receive corrupted messages and take action at the same time. The controller will have time to deal with all impacted aircraft.	Rare	Requirements for ensuring authenticity and protecting message integrity	Occasional
DLS	Services running with unnecessary privileges	Corruption of data	The situation will develop slowly: not all aircraft will receive corrupted messages and take action at the same time. The controller will have time to deal with all impacted aircraft.	Rare	The allocation and use of privileges shall be restricted and controlled	Occasional

Table 5: FMVEA example

5 CONCLUSIONS

The objective of this paper was the definition of a new methodology for carrying out safety and security risk assessment in air traffic control domain, harmonising both safety and security through the use of standard concepts and methodologies from both disciplines and showing how they interact in every stage of the life cycle. Both Safety and Security Requirements can be identified at design phase, considering areas of synergy and potential conflicts, and highlighting cost-effectiveness opportunities. For demonstrative purposes, the methodology has been applied to the real case study of approach and landing flight phases scenario, with a special focus on Controller-Pilot Data Link Communications systems.

6 ACKNOWLEDGEMENTS AND REFERENCES

The research leading to these results is carried out with the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks Programme of the European Commission – Directorate-General Home Affairs (Registration number HOME/2010/CIPS/AG/030, DORATHEA Project).

REFERENCES

[1] UK Centre for the Protection of National Infrastructure (CPNI), *Cyber Security in Civil Aviation*, 2012.

[2] Richard Paradis, Bambi Tran, *Balancing Security/Safety and Sustainability Objectives*, National Institute of Building Sciences, 2010.

[3] Thomas Novak, Andreas Gerstinger, *Safety- and Security-Critical Services in Building Automation and Control Systems*, IEEE Transactions on Industrial Electronics, vol. 57, no. 11, November 2010.

[4] IEC 15408, *Information Technology-Security Technique-Evaluation Criteria for IT Security*, 2005.

[5] IEC 61508, *Functional Safety of Electric/Electronic/Programmable Electronic Safety-Related Systems*, 1998.

[6] EUROCONTROL, *Air Navigation System Safety Assessment Methodology*, Ed. 2.1, 2006.

[7] EUROCONTROL, *EUROCONTROL Safety Regulatory Requirement ESARR4 Risk Assessment and Mitigation in ATM*, Ed. 1.0, 2001.

[8] F. Matarese, P. Montefusco, P. Altieri, J. Neves, A. Rocha, *Development of a Security Risk Assessment Methodology to enhance Security Awareness in ATM*, Avionics Europe Conference & Exhibition 2013.

[9] EUROCONTROL, *Deliverable 16.02.03 – SESAR ATM Security Risk Assessment Method*, Ed.01.01, SESAR WP16.2 ATM Security.

[10] ICAO, *Manual of Air Traffic Services Data Link Applications,* First Edition, 1999.